REMARKS

This application contains claims 1-69. Claims 9, 12, 17-19, 21-32, 34 and 36-45 have been canceled without prejudice. Claims 1, 2, 6, 10, 13-15, 20, 33, 35, 46 and 48-52 have been amended, and new claims 53-69 are hereby added. No new matter has been introduced. Reconsideration is respectfully requested.

Claims 12, 46 and 48 were objected to for informalities. Claim 12 has been canceled. Applicant has amended claims 46 and 48 to correct the informalities noted by the Examiner, and has also corrected minor errors in a number of the other original claims.

Claims 20 and 24 were rejected under 35 U.S.C. 112 for defects in antecedence. Applicant has amended claim 20 to correct the defect. Claim 24 has been canceled. Thus, all the claims in this application are now believed to meet the requirements of 35 U.S.C. 112.

Claims 1-52 were provisionally rejected for obviousness-type double patenting over the claims in U.S. patent applications 10/774,169 and 11/045,001. Applicant submits herewith a terminal disclaimer with respect to these two applications. Accordingly, Applicant respectfully submits that the double patenting rejection should be withdrawn.

Claims 1-52 were rejected under 35 U.S.C. 102(e) over Jungck (U.S. Patent 6,829,654). Applicant has amended independent claims 1, 46 and 49 in order to clarify the distinction of the present invention over Jungck. Independent claims 17, 21, 25, 27, 32 and 34, as well as some of the original dependent claims, have been canceled without prejudice in order to simplify and expedite prosecution of this application. Some of the remaining dependent claims have been amended for proper dependence in view of the amendments and cancellation of

other claims or otherwise to clarify claim language and correct informalities.

Jungck describes apparatus and methods for enhancing network infrastructure using edge servers and edge caches. The edge servers may also be used to detect malicious or otherwise unauthorized data transmissions (abstract). The edge server includes a request interceptor, a request filter and a request transmitter (col. 1, line 62 - col. 2, line 9). The function of the request filter is to determine whether the traffic it is monitoring is associated with a subscribing/affiliated server and whether it originated downstream or upstream from the server. Packets originating from upstream are preferably eradicated (col. 29, lines 25-39). The edge server can also monitor data transmission generated by clients for malicious program code (col. 28, lines 51-57) and can identify the originating client in a DDOS attack (col. 29, lines 3-7).

Claim 1 recites a method of responding to an overload condition, in which a first set of network elements diverts traffic destined for a victim to a second set of network elements. The second set filters the diverted traffic and selectively passes a portion of the traffic to the victim. The claim has been amended to state that the diversion of the traffic by the first set of network elements is initiated in response to detecting an anomalous traffic condition. This feature of the present invention was recited, in part, in claim 12 as filed (now canceled) and is described in detail in the specification. (See, for example, paragraphs 248, 252, 253 in the published version of this application, US 2002/0083175.) The inventors have found this feature to be critically important, since it permits the computing resources of the guards to be focused where they are actually needed.

Jungck neither teaches nor suggests the notion of initiating diversion of traffic responsively to detecting an anomalous traffic condition. His diversion evidently operates at all times and is not dependent on particular traffic conditions. On the contrary: for Jungck's edge caching methods to work optimally for their intended purpose, his edge servers should be operational to intercept and filter traffic at all times.

Thus, claim 1 as amended is believed to be patentable over Jungck. In view of the patentability of claim 1, dependent claims 2-8, 10, 11, 13-16, 20, 33 and 35 are also believed to be patentable.

Independent claim 46 recites a network element for use in protecting against an overload condition. The network element comprises an input, a filter for blocking traffic originating from a suspect source, a statistics module, and an output. The claim has been amended to clarify that the statistics module performs a statistical analysis of diverted traffic so as to detect an anomalous pattern of a flow associated with at least one source address. The filter blocks at least a portion of the data packets having such a source address. These functions of the network element are described particularly in paragraphs 295, 316 and 341-344 of the specification.

Jungck neither teaches nor suggests the use of a statistics module to detect anomalous flow patterns. In rejecting claim 46, the Examiner cited passages in cols. 28 and 29 of Jungck. These passages relate to detecting malicious program code (col. 28, lines 51-53) and identifying data packets whose origin address could not have come from a downstream network or affiliated POP (col. 28, lines 57-60). These functions of Jungck's edge router relate solely to particular characteristics (i.e., origin address or program code content) of individual packets. Jungck make no mention of statistical analysis

or of anomalous traffic flow patterns as required by amended claim 46. Indeed, statistical analysis would have no meaning with respect to the individual packet characteristics the Jungck mentions. Therefore, claim 46, as amended, is believed to be patentable over Jungck, as are claims 47 and 48, which depend from claim 46.

Independent claim 49 recites a system for use in protecting against an overload condition on a network. The system comprises one or more "guards," which comprise an input, a filter for selectively blocking traffic originating from a suspect source, a statistics module, and an output. One or more "diverters" selective divert to the guards traffic otherwise destined for a victim. The claim has been amended, in like fashion to claim 1, to recite that the diversion of traffic by the diverters is initiated responsively to detection of an anomalous traffic condition. As explained above in reference to claim 1, Jungck neither teaches nor suggests this sort of conditional initiation of traffic diversion. Therefore, claim 49, as amended, is believed to be patentable over Jungck, as are claims 50-52, which depend from claim 49.

New dependent claims 53-55 depend (directly or indirectly) from claim 1 and recite further aspects of the present invention that distinguish it over the prior art. Claim 53 recites that all of the traffic destined for the victim is diverted upon detecting an anomalous traffic condition. This claim is supported literally in the specification in paragraph 253. In Jungck's system, by contrast, a request filter 606 pre-filters traffic before the traffic is intercepted (col. 29, lines 22-23), and only some of the traffic is then handed off to the edge cache (col. 29, lines 46-55).

Claim 54 recites that an expected traffic pattern is learned while the victim is not under attack, and the anomalous traffic condition is detected when the traffic is determined to differ from the expected pattern. This

function is described in paragraphs 342-343 of the specification. It is neither taught nor suggested by Jungck.

Claim 55 recites that diversion is effected by a network switch, which routes traffic to the victim through a first port while the victim is not under attack. To initiate diversion under attack conditions, the network switch is instructed to route traffic destined for the victim through a second port that is coupled to one of the second set of network elements. The support for this claim in the specification and its distinction over Jungck are explained below with reference to independent claim 65.

New independent claim 56 recites a method of responding to an overload condition, which operates on similar principles to the network element recited in amended claim 46: A statistical analysis of diverted traffic is performed so as to detect an anomalous flow pattern associated with a source address, and at least a portion of the data packets having the source address is then prevented from reaching the victim. As explained above in reference to claim 46, Jungck neither teaches nor suggests this sort of statistical analysis. Therefore, claim 56 is believed to be patentable for the reasons explained above. In view of the patentability of claim 56, dependent claims 57-64 are also believed to be patentable.

Claim 57 recites that the statistical analysis is performed by learning an expected traffic pattern while the victim is not under attack, and then determining that the anomalous traffic pattern differs from the expected traffic pattern. This feature of the present invention is described in the specification in paragraphs 342-343. Even if Jungck were considered, for the sake of argument, to disclose some sort of statistical analysis, he makes no suggestion of learning an expected traffic pattern

while a victim is not under attack and then detecting a difference from the expected traffic pattern as recited in this claim.

Claims 58-65 restate additional features of the present invention that were recited in the claims as filed or are described in the specification (see particularly paragraphs 292-295). These added features, in conjunction with the statistical analysis recited in claim 56, are neither taught nor suggested by Jungck.

New independent claim 66 recites a method of responding to an overload condition at a victim network element. The victim is coupled to receive traffic from a network via a first port of a network switch. The network switch is actuated to divert the traffic destined for the victim to a second port, to which a guard machine is coupled. The guard machine filters the diverted traffic and selectively passes at least a portion of the filtered traffic to the victim. The configuration of routers (R0-R8) and guards (G0-G3) that carry out this method is shown in Figure 1 of the present patent application, and the method is described in paragraphs 248-250.

Jungck's edge servers 602 do not perform this sort of diversion. As shown in Jungck's Figs. 6 and 6A, for example, the functions of request filtering, interception, and proxy server are all carried out within the edge server. The edge servers always transmit traffic to the subscribing servers through the same ports. Jungck neither teaches nor suggests that such traffic might be diverted to a guard machine on a different port, for filtering and selective transmission to a victim, as required by claim 65. When Jungck's edge servers do hand requests off to an edge cache 604, the edge cache satisfies the request itself. The edge cache does not filter and pass the request on to the subscribing server (col. 29, lines 46-50), as would be

required by the method of claim 65. Thus, claim 65 is believed to be patentable over Jungck.

In view of the patentability of claim 66, new dependent claims 67-69 are also believed to be patentable. Claims 67 and 68 recite further features and functions of the network switches and guard machines shown in Fig. 1. Claim 69 recites performing statistical analysis, as in claim 56.

Applicant has studied the additional reference made of record by the Examiner, and believes all the claims currently pending in the application to be patentable over this reference, whether it is taken individually or in any combination.

Applicant believes the amendments and remarks stated above to be fully responsive to all of the objections and grounds of rejection raised by the Examiner. In view of these amendments and remarks, all the claims in the present patent application are believed to be in condition for allowance. Prompt notice to this effect is requested.

The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 141449, under Order No. 103376-3.

Dated: 3/20/06

Respectfully submitted,

By _____

David J. Powsner
Registration No.: 31,868
NUTTER MCCLENNEN & FISH LLP
World Trade Center West
155 Seaport Boulevard
Boston, Massachusetts 02210-2604
617) 439-2717
617) 310-9194 (Fax)
Attorney for Applicant